UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/589,221	08/11/2006	Masashi Watanabe	026893-001200US	5777

20350 7590 12/02/2009

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
12/02/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/589,221	WATANABE, MASASHI	
	Examiner	Art Unit	
	ARAVIND K. MOORTHY	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 January 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,13-33,36-52,55-69 and 72-97* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,13-33,36-52,55-69 and 72-97* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 August 2006* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the communications filed on 30 January 2008.

2. Claims 1-10, 13-33, 36-52, 55-69 and 72-97 are pending in the application.

3. Claims 1-10, 13-33, 36-52, 55-69 and 72-97 have been rejected.

4. Claims 11, 12, 34, 35, 53, 54, 70 and 71 have been cancelled in a preliminary amendment.

Information Disclosure Statement

5. The examiner has considered the information disclosure statement (IDS) filed on 11 August 2006 and 30 January 2008.

Drawings

6. The drawings are objected to because the drawings contain the label "SUBSTITUTE SHEET (RULE 26)". Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner,

the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 2, are rejected under 35 U.S.C. 102(e) as being anticipated by Tehranchi U.S. Patent No. 7,242,772 B1.

As to claim 1, Tehranchi discloses a method for cryptographically processing data, the method comprising:

receiving a plurality of data segments (i.e. data blocks) [column 7, lines 40-52];

selecting a set of encryption information for a current data segment to be encrypted based on data contained in a predetermined portion (i.e. synchronization index) of the current data segment (i.e. Key and synchronization generator generates an index that associates each generated encryption key with its corresponding data block) [column 7, lines 40-52];

encrypting the current data segment using the set of encryption information selected for the current data segment [column 9, lines 39-65]; and

repeating the selecting and the encrypting for subsequent data segments [column 9, lines 39-65].

As to claim 2, Tehranchi discloses that the selecting comprising:

changing at least one of an encryption algorithm, an encryption key, and an encryption parameter for each current data segment based on the data contained in the predetermined portion of the current data segment (i.e. each frame can use a different encryption key and algorithm) [column 9, lines 24-38].

As to claim 6, Tehranchi discloses that the predetermined portion comprises:

a first predetermined portion for selecting a first set of encryption information, the first set comprising a first encryption algorithm, a first encryption key, and optionally a first encryption parameter (i.e. each frame can use a different encryption key and algorithm) [column 9, lines 24-38]; and

a second predetermined portion for selecting a second set of encryption information, the second set comprising a second encryption algorithm, a second encryption key, and optionally a second encryption parameter (i.e. each frame can use a different encryption key and algorithm) [column 9, lines 24-38].

As to claim 7, Tehranchi discloses that the receiving comprises:

receiving a data stream including a plurality of data packets, each data packet corresponding to a data segment [column 12, lines 41-58].

As to claim 9, Tehranchi discloses that the first predetermined portion is an Internet Protocol (IP) header of the data packet [column 11, lines 50-65].

As to claim 10, Tehranchi discloses that the second predetermined portion is either one of:

a selected portion of a data field of the data packet (i.e. header field) [column 11, lines 50-65];

a Transmission Control Protocol (TCP) header of the data packet; and

a User Datagram Protocol (UDP) header of the data packet.

As to claim 15, Tehranchi discloses the method of claim 6, further comprising:

encrypting the second predetermined portion using the first set of encryption information (i.e. synchronization index) [column 10, lines 14-34].

As to claim 16, Tehranchi discloses the method of claim 15, further comprising:

encrypting the remaining portion of the data segment using the second set of encryption information (i.e. synchronization index) [column 10, lines 14-34].

As to claim 17, Tehranchi discloses the method of claim 16, further comprising:

generating an encrypted data segment for each of the original data segments, the encrypted data segment having a first predetermined portion (i.e. frame), a second predetermined portion (i.e. a second frame), and a remaining portion (i.e. remaining frame), the first predetermined portion containing the original data in the corresponding first predetermined portion of the original data segment, the second predetermined portion containing the encrypted data of the corresponding second predetermined portion of the original data segment, and the remaining portion containing the encrypted data of the corresponding remaining portion of the original data segment [column 9 line 24 to column 10 line 13].

As to claim 18, Tehranchi discloses the method of claim 17, further comprising:

transmitting a plurality of encrypted data segments as a stream of encrypted data [column 6 line 57 to column 7 line 6].

As to claim 20, Tehranchi discloses the method of claim 17, further comprising:

receiving the encrypted data including a plurality of encrypted data segments [column 9, lines 39-65];

selecting, for each encrypted data segment, a first set of encryption information based on data contained in the first predetermine portion of the encrypted data segment [column 9, lines 39-65];

decrypting the encrypted data contained in the second predetermined portion of each encrypted data segment using the first set of encryption information selected for the encrypted data segment [column 9, lines 39-65];

selecting, for each encrypted data segment, a second set of encryption information based on the decrypted data of the second predetermined portion [column 9, lines 39-65]; and

decrypting the remaining portion of each encrypted data segment using the second set of encryption information selected for the encrypted data segment [column 9, lines 39-65].

As to claim 25, Tehranchi discloses a method for cryptographically processing data, the method comprising:

receiving a plurality of encrypted data segments, each of the encrypted data segments having a predetermined portion [column 9, lines 39-65];

selecting a set of encryption information for a current encrypted data segment to be decrypted based on data contained in the predetermined portion of the current encrypted data segment [column 9, lines 39-65];

decrypting the current encrypted data segment using the encryption information selected for the current encrypted data segment [column 9, lines 39-65]; and

repeating the selecting and the decrypting for subsequent encrypted data segments [column 9, lines 39-65].

As to claim 29, Tehranchi discloses the method of claim 25, wherein the predetermined portion comprises:

a first predetermined portion for selecting a first set of encryption information, the first set comprising a first encryption algorithm, a first encryption key, and optionally a first encryption parameter [column 10, lines 14-34]; and

a second predetermined portion for selecting a second set of encryption information, the second set comprising a second encryption algorithm, a second encryption key, and optionally a second encryption parameter [column 10, lines 14-34].

As to claim 30, Tehranchi discloses the method of claim 29, wherein the receiving comprises:

receiving an encrypted data stream including a plurality of encrypted data packets, each encrypted data packet corresponding to an encrypted data segment [column 9, lines 24-38].

As to claim 32, Tehranchi discloses that the first predetermined portion is an Internet Protocol (IP) header of the data packet [column 11, lines 50-65].

As to claim 33, Tehranchi discloses that the second predetermined portion is either one of:

a selected portion of a data field of the data packet (i.e. header field) [column 11, lines 50-65];

a Transmission Control Protocol (TCP) header of the data packet; and

a User Datagram Protocol (UDP) header of the data packet.

As to claim 38, Tehranchi discloses that data contained in the second predetermined portion of the encrypted data segment has been encrypted using the first set of encryption information [column 9, lines 39-65].

As to claim 39, Tehranchi discloses that data contained in the remaining portion of the encrypted data segment has been encrypted using the second set of encryption information [column 9, lines 39-65].

As to claim 40, Tehranchi discloses an apparatus for cryptographically processing data, comprising:

an input buffer adapted to receive data including a plurality of data segments (i.e. data blocks) [column 7, lines 40-52];

an encryption module adapted to encrypt each data segment [column 9, lines 39-65];

a controller coupled to the input buffer and the encryption module, the controller being adapted to select a set of encryption information for a current

data segment to be encrypted based on data contained in a predetermined portion of the current data segment (i.e. Key and synchronization generator generates an index that associates each generated encryption key with its corresponding data block) [column 7, lines 40-52]; and

an output buffer coupled to the controller and the encryption module, the output buffer being adapted to output encrypted data including a plurality of encrypted data segments [column 9, lines 39-65].

As to claim 41, Tehranchi discloses that the controller changes at least one of an encryption algorithm, an encryption key, and an encryption parameter for each data segment (i.e. each frame can use a different encryption key and algorithm) [column 9, lines 24-38].

As to claim 42, Tehranchi discloses the apparatus of claim 40, wherein the encryption module comprises:

a plurality of encryption engines, each encryption engine corresponding to a respective encryption algorithm different from each other [column 9 line 66 to column 10 line 13].

As to claim 43, Tehranchi discloses the apparatus of claim 40, wherein the encryption module further comprises:

a data buffer coupled to each of the plurality of encryption engines (i.e. memory buffer) [column 7, lines 53-57].

As to claim 44, Tehranchi discloses the apparatus of claim 40, wherein the controller comprises:

a data selector adapted to select a predetermined portion of each data segment [column 9, lines 39-65];

an encryption selector coupled with the data selector, adapted to select a set of encryption information in accordance with data contained in the predetermined portion, the set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter [column 9, lines 39-65]; and

an encryption controller adapted to select and activate an encryption engine based on the encryption information [column 9, lines 39-65].

As to claim 48, Tehranchi discloses that the predetermined portion of each data segment comprises: a first predetermined portion; and a second predetermined portion (i.e. different frames) [column 9, lines 24-38].

As to claim 49, Tehranchi discloses that the plurality of data segments are data packets in a data stream [column 6 line 57 to column 7 line 6].

As to claim 51, Tehranchi discloses that the first predetermined portion is an Internet Protocol (IP) header of the data packet [column 11, lines 50-65].

As to claim 52, Tehranchi discloses the apparatus of claim 51, wherein the second predetermined portion is either one of:

a selected portion of a data field of the data packet (i.e. header field) [column 11, lines 50-65];

a Transmission Control Protocol (TCP) header of the data packet; and

a User Datagram Protocol (UDP) header of the data packet.

As to claim 57, Tehranchi discloses the apparatus of claim 48, wherein the controller comprises:

a first encryption table for selecting the first set of encryption information based on data contained in the first predetermined portion (i.e. as illustrated in figure 3); and

a second encryption table for selecting the second set of encryption information based on data contained in the second predetermined portion (i.e. as illustrated in figure 4).

As to claim 58, Tehranchi discloses an apparatus for cryptographically processing data, comprising:

an input buffer adapted to receive a plurality of encrypted data segments, each of the encrypted data segments having a predetermined portion (i.e. memory buffer) [column 7, lines 53-57];

an encryption module adapted to decrypt each encrypted data segment [column 9, lines 39-65];

a controller coupled-to the input buffer and the decryption module, the controller being adapted to select a set of encryption information for a current encrypted data segment to be decrypted based on data contained in a predetermined portion of the current encrypted data segment [column 9 line 66 to column 10 line 13]; and

an output buffer coupled to the controller and the decryption module, the output buffer being adapted to output decrypted data including a plurality of decrypted data segments [column 9 line 66 to column 10 line 13].

As to claim 59, Tehranchi discloses the apparatus of claim 58, wherein the decryption module comprises:

a plurality of decryption engines, each decryption engine corresponding to a respective encryption algorithm different from each other [column 9 line 66 to column 10 line 13].

As to claim 60, Tehranchi discloses the apparatus of claim 58, wherein the decryption module further comprises:

a data buffer coupled to each of the plurality of decryption engines (i.e. memory buffer) [column 7, lines 53-57].

As to claim 61, Tehranchi discloses the apparatus of claim 58, wherein the controller comprises:

a data selector adapted to select a predetermined portion of each encrypted data segment [column 9 line 66 to column 10 line 13];

a decryption selector coupled with the data selector, adapted to select a set of decryption information in accordance with data contained in the predetermined portion, the set of decryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter [column 9 line 66 to column 10 line 13]; and

a decryption controller adapted to select and activate a decryption engine based on the encryption information [column 9 line 66 to column 10 line 13].

As to claim 65, Tehranchi discloses the apparatus of claim 58, wherein the predetermined portion of each data segment comprises:

a first predetermined portion [column 9, lines 24-38]; and

a second predetermined portion [column 9, lines 24-38].

As to claim 66, Tehranchi discloses that the plurality of data segments are data packets in a data stream [column 6 line 57 to column 7 line 6].

As to claim 68, Tehranchi discloses that the first predetermined portion is an Internet Protocol (IP) header of the data packet [column 11, lines 50-65].

As to claim 69, Tehranchi discloses the apparatus of claim 68, wherein the second predetermined portion is either one of:

a selected portion of a data field of the data packet (i.e. header field) [column 11, lines 50-65];

a Transmission Control Protocol (TCP) header of the data packet; and

a User Datagram Protocol (UDP) header of the data packet.

As to claim 74, Tehranchi discloses the apparatus of claim 58, wherein the controller comprises:

a first encryption table for selecting the first set of decryption information based on data contained in the first predetermined portion (i.e. as illustrated in figure 3); and

a second encryption table for selecting the second set of decryption information based on data contained in the second predetermined portion (i.e. as illustrated in figure 4).

As to claim 75, Tehranchi discloses an apparatus for cryptographically processing data, the apparatus comprising:

means for receiving a plurality of data segments (i.e. data blocks) [column 7, lines 40-52];

means for selecting a set of encryption information for a current data segment to be encrypted based on data contained in a predetermined portion (i.e. synchronization index) of the current data segment (i.e. Key and synchronization generator generates an index that associates each generated encryption key with its corresponding data block) [column 7, lines 40-52];

means for encrypting the current data segment using the set of encryption information selected for the current data segment [column 9, lines 39-65]; and

means for allowing the means for selecting and the means for encrypting to operate on subsequent data segments [column 9, lines 39-65].

As to claim 76, Tehranchi discloses that the means for selecting changes at least one of an encryption algorithm, an encryption key, and an encryption parameter for each data segment based on the data contained in the predetermined portion (i.e. each frame can use a different encryption key and algorithm) [column 9, lines 24-38].

As to claim 80, Tehranchi discloses that the predetermined portion comprises:

a first predetermined portion for selecting a first set of encryption information, the first set comprising a first encryption algorithm, a first encryption key, and optionally a first encryption parameter [column 9, lines 39-65]; and

a second predetermined portion for selecting a second set of encryption information, the second set comprising a second encryption algorithm, a second encryption key, and optionally a second encryption parameter [column 9, lines 39-65].

As to claim 81, Tehranchi discloses the apparatus of claim 80, further comprising:

means for encrypting the second predetermined portion using the first set of encryption information [column 9, lines 39-65].

As to claim 82, Tehranchi discloses the apparatus of claim 81, further comprising:

means for encrypting the remaining portion of the data segment using the second set of encryption information [column 9, lines 39-65].

As to claim 83, Tehranchi discloses the apparatus of claim 82, further comprising:

means for generating an encrypted data segment for each of the original data segments, the encrypted data segment having a first predetermined portion (i.e. first frame), a second predetermined portion (i.e. second frame), and a remaining portion (i.e. remaining frames), the first predetermined portion containing the original data in the corresponding first predetermined portion of the original data segment, the second predetermined portion containing the encrypted data of the corresponding second predetermined portion of the original data segment, and the remaining portion containing the encrypted data of the

corresponding remaining portion of the original data segment [column 9 line 24 to column 10 line 13].

As to claim 84, Tehranchi discloses the apparatus of claim 83, further comprising:

means for transmitting a plurality of encrypted data segments as a stream of encrypted data [column 6 line 57 to column 7 line 6].

As to claim 86, Tehranchi discloses the apparatus of claim 83, further comprising:

means for receiving the encrypted data including a plurality of encrypted data segments [column 9 line 39 to column 10 line 13];

means for selecting, for each encrypted data segment, a first set of encryption information based on data contained in the first predetermine portion of the encrypted data segment [column 9 line 39 to column 10 line 13];

means for decrypting the encrypted data contained in the second predetermined portion of each encrypted data segment using the first set of encryption information selected for the encrypted data segment [column 9 line 39 to column 10 line 13];

means for selecting, for each encrypted data segment, a second set of encryption information based on the decrypted data of the second predetermined portion [column 9 line 39 to column 10 line 13]; and

means for decrypting the remaining portion of each encrypted data segment using the second set of encryption information selected for the encrypted data segment [column 9 line 39 to column 10 line 13].

As to claim 91, Tehranchi discloses an apparatus for cryptographically processing data, the apparatus comprising:

means for receiving a plurality of encrypted data segments, each of the encrypted data segments having a predetermined portion [column 9 line 39 to column 10 line 13];

means for selecting a set of encryption information for a current encrypted data segment to be decrypted based on data contained in the predetermined portion of the current encrypted data segment [column 9 line 39 to column 10 line 13];

means for decrypting the current encrypted data segment using the encryption information selected for the current encrypted data segment [column 9 line 39 to column 10 line 13]; and

means for allowing the means for selecting and the means for decrypting to operate on subsequent encrypted data segments [column 9 line 39 to column 10 line 13].

As to claim 95, Tehranchi discloses the apparatus of claim 91, wherein the predetermined portion comprises:

a first predetermined portion for selecting a first set of encryption information, the first set comprising a first encryption algorithm, a first encryption key, and optionally a first encryption parameter [column 9 line 39 to column 10 line 13]; and

a second predetermined portion for selecting a second set of encryption information, the second set comprising a second encryption algorithm, a second encryption key, and optionally a second encryption parameter [column 9 line 39 to column 10 line 13].

As to claim 96, Tehranchi discloses that data contained in the second predetermined portion of the encrypted data segment has been encrypted using the first set of encryption information [column 10, lines 14-34].

As to claim 97, Tehranchi discloses that data contained in the remaining portion of the encrypted data segment has been encrypted using the second set of encryption information [column 10, lines 14-34].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 3-5, 21-24, 26-28, 45-47, 62-64, 77-79, 87-90 and 92-94 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tehranchi U.S. Patent No. 7,242,772 B1 as applied to claims 1, 20, 25, 40, 58, 75, 86 and 91 above, and further in view of Hall et al US 2005/0074116 A1 (hereinafter Hall).

As to claims 3 and 4, Tehranchi does not teach generating, for each current data segment, a value from data contained in the predetermined portion of the current data segment. Tehranchi does not teach selecting a set of encryption information associated with the generated value, the

set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter. Tehranchi does not teach that the generating a value comprises hashing the data contained in the predetermined portion using a hash key.

Hall teaches generating a checksum value by imputing at least one of a plurality of plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys [0017-0019].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that a value would have been generated from data contained in the predetermined portion of the current data segment. A set of encryption information would have been selected associated with the generated value. The set of encryption information would have included an encryption algorithm, an encryption key, and optionally an encryption parameter. The value would have been generated by hashing the data contained in the predetermined portion using a hash key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Hall because it provides a universal hash for plaintext-aware encryption that has low-complexity and does not require a large amount of key material [0006].

As to claim 5, Tehranchi teaches providing an encryption table containing: an encryption type identifier; an encryption key for the encryption type; and an encryption parameter [column 9 line 66 to column 10 line 13].

Tehranchi does not teach that each entry is associated with a generate value.

Hall teaches generating a checksum value [0017-0019].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that the checksum value would have been associated with entries of the encryption table.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Hall because it provides a universal hash for plaintext-aware encryption that has low-complexity and does not require a large amount of key material [0006].

As to claims 21 and 22, Tehranchi does not teach generating a first value from the original data contained in the first predetermined portion of the encrypted data segment. Tehranchi does not teach hashing the data contained in the first predetermined portion using a first hash key.

Hall teaches generating a checksum value by imputing at least one of a plurality of plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys [0017-0019].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that a first value would have been generated from the original data contained in the first predetermined portion of the encrypted data segment. The data would have been hashed contained in the first predetermined portion using a first hash key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Hall because it provides a

universal hash for plaintext-aware encryption that has low-complexity and does not require a large amount of key material [0006].

As to claims 23 and 24, Tehranchi does not teach generating a second value from the decrypted data of the second predetermined portion of the encrypted data segment. Tehranchi does not teach hashing the decrypted data of the second predetermined portion using a second hash key.

Hall teaches generating a checksum value by imputing at least one of a plurality of plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys [0017-0019].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that a second value would have been generated from the decrypted data of the second predetermined portion of the encrypted data segment. The decrypted data would have been hashed of the second predetermined portion using a second hash key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Hall because it provides a universal hash for plaintext-aware encryption that has low-complexity and does not require a large amount of key material [0006].

As to claims 26 and 27, Tehranchi does not teach generating, for each current data segment, a value from data contained in the predetermined portion of the current data segment. Tehranchi does not teach selecting a set of encryption information associated with the generated value, the set of encryption information including an encryption algorithm, an encryption key,

and optionally an encryption parameter. Tehranchi does not teach that the generating a value comprises hashing the data contained in the predetermined portion using a hash key.

Hall teaches generating a checksum value by imputing at least one of a plurality of plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys [0017-0019].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that a value would have been generated from data contained in the predetermined portion of the current data segment. A set of encryption information would have been selected associated with the generated value. The set of encryption information would have included an encryption algorithm, an encryption key, and optionally an encryption parameter. The value would have been generated by hashing the data contained in the predetermined portion using a hash key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Hall because it provides a universal hash for plaintext-aware encryption that has low-complexity and does not require a large amount of key material [0006].

As to claim 28, Tehranchi teaches providing an encryption table containing: an encryption type identifier; an encryption key for the encryption type; and an encryption parameter [column 9 line 66 to column 10 line 13].

Tehranchi does not teach that each entry is associated with a generate value.

Hall teaches generating a checksum value [0017-0019].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that the checksum value would have been associated with entries of the encryption table.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Hall because it provides a universal hash for plaintext-aware encryption that has low-complexity and does not require a large amount of key material [0006].

As to claims 45 and 46, Tehranchi does not teach a value generator coupled to the data selector, adapted to generate a value from the data contained in the predetermined portion. Tehranchi does not teach that the value generator is adapted to hash the data contained in the predetermined portion using a hash key.

Hall teaches generating a checksum value by imputing at least one of a plurality of plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys [0017-0019].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that a value generator would have been coupled to the data selector, adapted to generate a value from the data contained in the predetermined portion. The value generator would have been adapted to hash the data contained in the predetermined portion using a hash key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Hall because it provides a

universal hash for plaintext-aware encryption that has low-complexity and does not require a large amount of key material [0006].

As to claim 47, Tehranchi does not teach that the encryption controller comprises an encryption table containing: an encryption type identifier; an encryption key for the encryption type; and an encryption parameter, for each entry associated with a generated value.

Tehranchi does not teach that each entry is associated with a generate value.

Hall teaches generating a checksum value [0017-0019].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that the checksum value would have been associated with entries of the encryption table.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Hall because it provides a universal hash for plaintext-aware encryption that has low-complexity and does not require a large amount of key material [0006].

As to claims 62 and 63, Tehranchi does not teach a value generator coupled to the data selector, adapted to generate a value from the data contained in the predetermined portion. Tehranchi does not teach that the value generator is adapted to hash the data contained in the predetermined portion using a hash key.

Hall teaches generating a checksum value by imputing at least one of a plurality of plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys [0017-0019].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that a value generator would have been coupled to the data selector, adapted to generate a value from the data contained in the predetermined portion. The value generator would have been adapted to hash the data contained in the predetermined portion using a hash key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Hall because it provides a universal hash for plaintext-aware encryption that has low-complexity and does not require a large amount of key material [0006].

As to claim 64, Tehranchi does not teach that the encryption controller comprises an encryption table containing: an encryption type identifier; an encryption key for the encryption type; and an encryption parameter, for each entry associated with a generated value.

Tehranchi does not teach that each entry is associated with a generate value.

Hall teaches generating a checksum value [0017-0019].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that the checksum value would have been associated with entries of the encryption table.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Hall because it provides a universal hash for plaintext-aware encryption that has low-complexity and does not require a large amount of key material [0006].

As to claims 77 and 78, Tehranchi does not teach generating, for each current data segment, a value from data contained in the predetermined portion of the current data segment. Tehranchi does not teach selecting a set of encryption information associated with the generated value, the set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter. Tehranchi does not teach that the generating a value comprises hashing the data contained in the predetermined portion using a hash key.

Hall teaches generating a checksum value by imputing at least one of a plurality of plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys [0017-0019].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that a value would have been generated from data contained in the predetermined portion of the current data segment. A set of encryption information would have been selected associated with the generated value. The set of encryption information would have included an encryption algorithm, an encryption key, and optionally an encryption parameter. The value would have been generated by hashing the data contained in the predetermined portion using a hash key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Hall because it provides a universal hash for plaintext-aware encryption that has low-complexity and does not require a large amount of key material [0006].

As to claim 79, Tehranchi teaches providing an encryption table containing: an encryption type identifier; an encryption key for the encryption type; and an encryption parameter [column 9 line 66 to column 10 line 13].

Tehranchi does not teach that each entry is associated with a generate value.

Hall teaches generating a checksum value [0017-0019].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that the checksum value would have been associated with entries of the encryption table.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Hall because it provides a universal hash for plaintext-aware encryption that has low-complexity and does not require a large amount of key material [0006].

As to claims 87 and 88, Tehranchi does not teach generating a first value from the original data contained in the first predetermined portion of the encrypted data segment. Tehranchi does not teach hashing the data contained in the first predetermined portion using a first hash key.

Hall teaches generating a checksum value by imputing at least one of a plurality of plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys [0017-0019].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that a first value would have been generated from the original data contained in the first predetermined portion of the encrypted

data segment. The data would have been hashed contained in the first predetermined portion using a first hash key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Hall because it provides a universal hash for plaintext-aware encryption that has low-complexity and does not require a large amount of key material [0006].

As to claims 89 and 90, Tehranchi does not teach generating a second value from the decrypted data of the second predetermined portion of the encrypted data segment. Tehranchi does not teach hashing the decrypted data of the second predetermined portion using a second hash key.

Hall teaches generating a checksum value by imputing at least one of a plurality of plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys [0017-0019].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that a second value would have been generated from the decrypted data of the second predetermined portion of the encrypted data segment. The decrypted data would have been hashed of the second predetermined portion using a second hash key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Hall because it provides a universal hash for plaintext-aware encryption that has low-complexity and does not require a large amount of key material [0006].

As to claims 92 and 93, Tehranchi does not teach generating, for each current data segment, a value from data contained in the predetermined portion of the current data segment. Tehranchi does not teach selecting a set of encryption information associated with the generated value, the set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter. Tehranchi does not teach that the generating a value comprises hashing the data contained in the predetermined portion using a hash key.

Hall teaches generating a checksum value by imputing at least one of a plurality of plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys [0017-0019].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that a value would have been generated from data contained in the predetermined portion of the current data segment. A set of encryption information would have been selected associated with the generated value. The set of encryption information would have included an encryption algorithm, an encryption key, and optionally an encryption parameter. The value would have been generated by hashing the data contained in the predetermined portion using a hash key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Hall because it provides a universal hash for plaintext-aware encryption that has low-complexity and does not require a large amount of key material [0006].

As to claim 94, Tehranchi does not teach that the encryption controller comprises an encryption table containing: an encryption type identifier; an encryption key for the encryption type; and an encryption parameter, for each entry associated with a generated value.

Tehranchi does not teach that each entry is associated with a generate value.

Hall teaches generating a checksum value [0017-0019].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that the checksum value would have been associated with entries of the encryption table.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Hall because it provides a universal hash for plaintext-aware encryption that has low-complexity and does not require a large amount of key material [0006].

9. Claims 8, 31, 50 and 67 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tehranchi U.S. Patent No. 7,242,772 B1 as applied to claims 7, 30, 49 and 66 above, and further in view of Robinson et al US 2006/0140197 A1 (hereinafter Robinson).

As to claim 8, Tehranchi does not teach that the first predetermined portion contains data for a first protocol layer, and the second predetermined portion contains data for a second protocol layer, wherein the first protocol layer is lower than the second protocol layer.

Robinson teaches a segment of data for a first protocol layer (i.e. network layer) [0045]. Robinson teaches a segment of data for a second protocol layer (i.e. transport layer) [0046]. The network layer is lower than the transport layer.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that the first predetermined portion would have contained data for a first protocol layer, and the second predetermined portion would have contained data for a second protocol layer, wherein the first protocol layer was lower than the second protocol layer.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Robinson because it provides a method for recovering data lost in a transmission and is useful for improving the reliabitly of data unit delivery [0002].

As to claim 31, Tehranchi does not teach that the first predetermined portion contains data for a first protocol layer, and the second predetermined portion contains data for a second protocol layer, wherein the first protocol layer is lower than the second protocol layer.

Robinson teaches a segment of data for a first protocol layer (i.e. network layer) [0045]. Robinson teaches a segment of data for a second protocol layer (i.e. transport layer) [0046]. The network layer is lower than the transport layer.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that the first predetermined portion would have contained data for a first protocol layer, and the second predetermined portion would have contained data for a second protocol layer, wherein the first protocol layer was lower than the second protocol layer.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Robinson because it provides

a method for recovering data lost in a transmission and is useful for improving the reliabitly of data unit delivery [0002].

As to claim 50, Tehranchi does not teach that the first predetermined portion contains data for a first protocol layer, and the second predetermined portion contains data for a second protocol layer, wherein the first protocol layer is lower than the second protocol layer.

Robinson teaches a segment of data for a first protocol layer (i.e. network layer) [0045]. Robinson teaches a segment of data for a second protocol layer (i.e. transport layer) [0046]. The network layer is lower than the transport layer.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that the first predetermined portion would have contained data for a first protocol layer, and the second predetermined portion would have contained data for a second protocol layer, wherein the first protocol layer was lower than the second protocol layer.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Robinson because it provides a method for recovering data lost in a transmission and is useful for improving the reliabitly of data unit delivery [0002].

As to claim 67, Tehranchi does not teach that the first predetermined portion contains data for a first protocol layer, and the second predetermined portion contains data for a second protocol layer, wherein the first protocol layer is lower than the second protocol layer.

Robinson teaches a segment of data for a first protocol layer (i.e. network layer) [0045]. Robinson teaches a segment of data for a second protocol layer (i.e. transport layer) [0046]. The network layer is lower than the transport layer.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that the first predetermined portion would have contained data for a first protocol layer, and the second predetermined portion would have contained data for a second protocol layer, wherein the first protocol layer was lower than the second protocol layer.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Robinson because it provides a method for recovering data lost in a transmission and is useful for improving the reliabitly of data unit delivery [0002].

10. Claims 13, 14, 19, 36, 37, 55, 56, 72, 73 and 85 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tehranchi U.S. Patent No. 7,242,772 B1 as applied to claims 6, 17, 29, 48, 58 and 83 above, and further in view of Tomori et al U.S. Patent No. 6,865,658 B2 (hereinafter Tomori).

As to claims 13 and 14, Tehranchi does not teach reading the plurality of data segments from corresponding sectors in a data storage device. Tehranchi does not teach that the first predetermined portion is a first selected portion in a sector in a data storage device, and the second predetermined portion is a second selected portion in the sector.

Tomori teaches storing and reading data segments from sectors in a data storage device [column 20 line 56 to column 21 line 2; column 24, lines 48-57].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that the plurality of data segments would have been read from corresponding sectors in a data storage device. The first predetermined portion would have been a first selected portion in a sector in a data storage device, and the second predetermined portion would have been a second selected portion in the sector.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Tomori because it provides the advantage of providing a data management system and data management method where data divided in units of a sector is stored together with data link information in a plurality of separately distributed sectors of a data storage region, so that the data storage region can be more efficiently utilized [column 16, lines 30-35].

As to claim 19, Tehranchi discloses storing a plurality of encrypted data segments on a data storage device [column 7 line 53 to column 8 line 6].

Tehranchi does not teach that each encrypted data segment corresponds to a respective data sector of the data storage device.

Tomori teaches storing and reading data segments from sectors in a data storage device [column 20 line 56 to column 21 line 2; column 24, lines 48-57].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that the plurality of encrypted data segments would have stored on a data storage device. Each encrypted segment would have corresponded to a respective data sector of the data storage device.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Tomori because it provides the advantage of providing a data management system and data management method where data divided in units of a sector is stored together with data link information in a plurality of separately distributed sectors of a data storage region, so that the data storage region can be more efficiently utilized [column 16, lines 30-35].

As to claims 36 and 37, Tehranchi does not teach reading the plurality of encrypted data segments from corresponding sectors in a data storage device. Tehranchi does not teach that the first predetermined portion is a first selected portion in a sector in a data storage device, and the second predetermined portion is a second selected portion in the sector.

Tomori teaches storing and reading data segments from sectors in a data storage device [column 20 line 56 to column 21 line 2; column 24, lines 48-57].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that the plurality of encrypted data segments would have been read from corresponding sectors in a data storage device. The first predetermined portion would have been a first selected portion in a sector in a data storage device, and the second predetermined portion would have been a second selected portion in the sector.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Tomori because it provides the advantage of providing a data management system and data management method where data divided in units of a sector is stored together with data link information in a plurality of

separately distributed sectors of a data storage region, so that the data storage region can be more efficiently utilized [column 16, lines 30-35].

As to claims 55 and 56, Tehranchi does not teach that the plurality of data segments are sectors in a data storage device. Tehranchi does not teach that the first predetermined portion is a first selected portion in a sector in a data storage device, and the second predetermined portion is a second selected portion in the sector.

Tomori teaches storing and reading data segments from sectors in a data storage device [column 20 line 56 to column 21 line 2; column 24, lines 48-57].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that the plurality of data segments would have been read from corresponding sectors in a data storage device. The first predetermined portion would have been a first selected portion in a sector in a data storage device, and the second predetermined portion would have been a second selected portion in the sector.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Tomori because it provides the advantage of providing a data management system and data management method where data divided in units of a sector is stored together with data link information in a plurality of separately distributed sectors of a data storage region, so that the data storage region can be more efficiently utilized [column 16, lines 30-35].

As to claims 72 and 73, Tehranchi does not teach that the plurality of data segments are sectors in a data storage device. Tehranchi does not teach that the first predetermined portion is a

first selected portion in a sector in a data storage device, and the second predetermined portion is a second selected portion in the sector.

Tomori teaches storing and reading data segments from sectors in a data storage device [column 20 line 56 to column 21 line 2; column 24, lines 48-57].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that the plurality of data segments would have been read from corresponding sectors in a data storage device. The first predetermined portion would have been a first selected portion in a sector in a data storage device, and the second predetermined portion would have been a second selected portion in the sector.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Tomori because it provides the advantage of providing a data management system and data management method where data divided in units of a sector is stored together with data link information in a plurality of separately distributed sectors of a data storage region, so that the data storage region can be more efficiently utilized [column 16, lines 30-35].

As to claim 85, Tehranchi discloses storing a plurality of encrypted data segments on a data storage device [column 7 line 53 to column 8 line 6].

Tehranchi does not teach that each encrypted data segment corresponds to a respective data sector of the data storage device.

Tomori teaches storing and reading data segments from sectors in a data storage device [column 20 line 56 to column 21 line 2; column 24, lines 48-57].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi so that the plurality of encrypted data segments would have stored on a data storage device. Each encrypted segment would have corresponded to a respective data sector of the data storage device.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Tehranchi by the teaching of Tomori because it provides the advantage of providing a data management system and data management method where data divided in units of a sector is stored together with data link information in a plurality of separately distributed sectors of a data storage region, so that the data storage region can be more efficiently utilized [column 16, lines 30-35].

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ARAVIND K. MOORTHY whose telephone number is (571)272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2431